

機密情報の無敵化

データ窃取・ノーウェアランサム対策ソフトウェア

DATA SEALED SAFER

DATA SEALED SAFERは機密性の高い暗号化技術を採用しているため、
万が一データ窃取の被害にあっても、
窃取された情報を無意味なものにすることができます。

DATA SEALED SAFERが必要な理由

① 企業の命を守る



データ窃取は企業の存亡の危機

データ窃取は企業の存亡に深刻な影響を及ぼす重大課題です。顧客の信頼やブランドイメージが損なわれ、法的責任や損害賠償が発生し、最悪の場合、企業の存続に関わる事態に発展することがあります。

② 変化をうながす



データ窃取対策が必須の時代

セキュリティ対策はコストではなく将来の利益を確保するための戦略的投資と考える必要があります。時代に対応する事業展開をするため、まずはデータ窃取対策から機密情報の取り扱い意識と働き方を変える必要があります。

③ これで戦える



データは盗られても信用は守る

サイバー攻撃を完全に防ぐことは不可能です。機密情報が盗まれても解読できないように高度な暗号化を備えたDATA SEALED SAFERでの暗号化はデータ窃取と信用失墜を防ぐ対策となります。

DATA SEALED SAFER の特徴

1 様々なデータを暗号化保護できる、 “国産”のファイル暗号化



- Microsoft Word、Excel、PowerPointや一太郎、PDFなどのオフィス系ファイル
- AutoCAD、CATIAなどのCAD系ファイル
- Visioなどの技術系ファイル
- Photoshop、動画などのマルチメディア系ファイルをはじめとするほとんどのファイルを暗号化可能。

※DATA SEALED SAFERの暗号化でファイルサイズが約1KB増加します。

2 Excel・Word等の主なアプリは自動復号/暗号化

利用機会の多い主なアプリケーション/ファイルは、DATA SEALED SAFERを暗号化後、通常の操作でファイルを開くことができます。編集終了後は、自動的に暗号化ファイルとして保存されます。

主なアプリケーション

PDF、Microsoft Office (Word、Excel、PowerPoint)
画像編集ソフト (ペイント)、エディタ (メモ帳、ワードパッド、秀丸エディタ、EmEditor、TeraPad、NoEditor)

3 優れたユーザビリティ

右クリックで暗号/復号

右クリックでファイルを個別でも複数まとめても暗号化できます。また、フォルダを選択することでフォルダ内のファイルをまとめて暗号化することもできます。

ファイル名・拡張子が変わらない

アイコンやファイル名や拡張子が変わらないため直感的に使用可能。マクロやリンクも暗号化前と同様に利用可能です。



4 高度な暗号技術を採用

電子政府推奨暗号リストに記載の 安全性・実装性能確認暗号技術

ファイル自体にセキュリティ機能を組み込むことで、ファイルに対する閲覧、編集、印刷等の操作を制御する技術。電子政府推奨暗号リストに記載の安全性・実装性能が確認された暗号技術であり、個人情報保護法で報告を要しない「高度な暗号化」技術を実現しました。

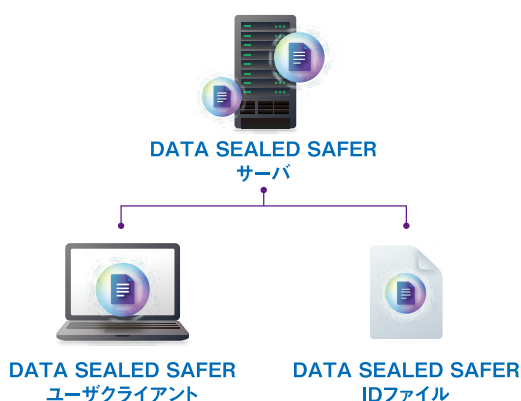
DATA SEALED SAFERで暗号化したデータは、
自社のDATA SEALED SAFER導入PCユーザ以外では解読できません。

Check!

AppCheck を
お使いの方・ご導入検討の方へ

DATA SEALED SAFERはランサムウェア対策セキュリティソフト「AppCheck」と同居を前提に設計しているため、コンフリクトを起こすことなく同居することができます。同居に必要な設定作業をする必要がありません。

システム構成・動作環境



DATA SEALED SAFER サーバ

サーバにアクセスするIDファイルの利用者情報に基づき暗号化と復号に必要な鍵を配信するプログラムです。

構成: PostgreSQLサーバ / DATA SEALED SAFERサーバ /
DATA SEALED SAFERマネージャクライアント

DATA SEALED SAFER ユーザクライアント

利用者のPCで動作するプログラムです。

DATA SEALED SAFER IDファイル

利用者が持つ鍵情報ファイルです。
暗号化ファイルを利用する際に必須
本人認証などを行う重要なファイルです。

動作環境 (ご用意いただく機器SPEC)

Windows Server 2016 (64bit)
Windows Server 2019 (64bit)
Windows Server 2022 (64bit)
Windows Server 2025 (64bit)
CPU Intel互換 2.0 GHz 2Core以上
メモリ 8GB以上
HDD 100GB以上

Windows 10 (32/64bit)
Windows 11 (64bit)
CPU Intel互換 2.0 GHz 2Core以上
メモリ 2GB以上
HDD 1GB以上

※DATA SEALED SAFERサーバとDATA SEALED SAFERクライアントで疎通できればWANでも使用可能

製品の詳細はこちらから

<https://www2.santec.com/dss/>



※記載の製品名などは、各社及び各団体の商標又は登録商標です。



santec Japan株式会社

本社 Tel: 0568-55-3654
〒485-0802 愛知県小牧市大草年上坂5823
東京オフィス Tel: 050-3110-3150
〒105-0013
東京都港区浜松町2-10-6PMO浜松町Ⅲ10F